UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/724,321	11/26/2003	Scott H. Robinson	P17409	1457

59796 7590 12/20/2010

INTEL CORPORATION
c/o CPA Global
P.O. BOX 52050
MINNEAPOLIS, MN 55402

EXAMINER	
YALEW, FIKREMARIAM A	
ART UNIT	PAPER NUMBER
2436	

NOTIFICATION DATE	DELIVERY MODE
12/20/2010	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

heather.l.adamson@intel.com

Office Action Summary	Application No.	Applicant(s)	
	10/724,321	ROBINSON ET AL.	
	Examiner	Art Unit	
	Fikremariam Yalew	2436	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *19 October 2010*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-33* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-33* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 10/19/2010 has been entered.

Response to Arguments

2. Applicant's arguments with respect to claims 1-33 have been considered but are not persuasive. The applicant argued that the prior art does not teach or suggest "executing a first instruction of a plurality of instruction in the instruction set architecture of the processor and a second instruction of the plurality of instruction in the instruction set architecture of the processor wherein execution of the first instruction causes the processor to read the encoded private-state data from the location, the second instruction causing to read the encoded private -state data from the storage and to produce decoded private-state data and store the decoded private state data in the processor. The examiner disagree and points out the combination of Kabushiki-Weidner-Ma teaches executing a first instruction of a plurality of instruction in the instruction set architecture of the processor wherein execution of the first instruction causes the processor to read the encoded private-state data from the location (See col.5.lines 1-23, col.10 lines 43-63,col.13 lines 6-15 (i.e., **the CPU/instruction decoder for execution & the overall decryption operation is therefore performed essentially simultaneously on at least two instructions & read/write accessing external memory**)) and a second instruction

of the plurality of instruction in the instruction set architecture of the processor(See col.5.lines 1-23(i.e., **the CPU/instruction decoder for execution & the overall decryption operation is therefore performed essentially simultaneously on at least two instructions**), the second instruction causing to read the encoded private -state data from the storage and to produce decoded private-state data and store the decoded private state data in the processor(See Fig 3 steps 305,310 ,Fig 7 and col.2.lines 2-6 and col.5.lines 1-23, col.10 lines 43-63,col.13 lines 6-15 (i.e., **receive multiple encrypted instruction into a buffer of a microcontroller from an external memory & decrypt the multiple encrypted instructions simultaneously using selected decryption algorithm**)).The examiner interpreted encrypted instruction as private-state data. In response to applicant's argument that there is no suggestion to combine the references, the examiner recognizes that obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. See In re Fine, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988) and In re Jones, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992). In this case, .It would modify in order to enhance security of the system by protecting state data from analysis (See Ma col.2 lines 3-5).

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and

the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 1-9 are rejected under 35 U.S.C. 103(a) as being unpatentable over by EP 1,126,356(Kabushiki Kaisha Toshiba Aug 22,2001) in view of Weidner et al(hereinafter referred as Weidner) US Patent No 5,987,572 and further in view of Hashimoto et al(hereinafter referred as Hashimoto) US 6,983,374 B2

5. As per claim 1: Hashimoto discloses a method for operating a data processing machine, comprising: a) applying by a processor an encoding process to private-state data, where the private-state data captures a state of the processor (See 0036(i.e., encryption/decryption unit being part of the processor (lines 2-5) and where the private-state data captures a state of the processor (lines 5-6)) and Fig 1 and 0067); b) writing, to a location in storage, said encoded private-state data (See 0036 lines 8-10), the location being one that is accessible to software that may be written for the processor(See 0094 lines 7-9);

Hashimoto does not explicitly disclose and c) reading by the software the private-state data from the storage using an instruction that causes the processor to apply a decoding process that can undo the encoding process.

However Weidner discloses c) reading by the software the private-state data from the storage using an instruction that causes the processor to apply a decoding process that can undo the encoding process (See col. 5 lines 12-32 and col. 4 lines 9-23)

Therefore it would have been obvious to one ordinary skill in the art at that time the invention was made to employ the teaching method of Weidner within Hashimoto method in order to enhance security of the system.

The combination of Weidner and Hashimoto does not explicitly teach by executing a first instruction of a plurality of instruction in the instruction set architecture of the processor, wherein execution of the first instruction causes the processor to read the encoded private-state data from the location and a second instruction of the plurality of instruction in the instruction set architecture of the processor, wherein execution of the second instruction causing to read the encoded private -state data from the storage and to produce decoded private-state data and store the decoded private state data in the processor.

Ma teaches using a first instruction of a plurality of instruction in the instruction set architecture of the processor wherein execution of the first instruction causes the processor to read the encoded private-state data from the location(See col.5.lines 1-23, col.10 lines 43-63,col.13 lines 6-15) and a second instruction of the plurality of instruction in the instruction set architecture of the processor wherein execution of the second instruction causes the processor to read the encoded private -state data from the storage and to produce decoded private-state data and store the decoded private state data in the processor(See Fig 3 steps 305,310, Fig 7 and col.2.lines 2-6 and col.5.lines 1-23, col.10 lines 43-63,col.13 lines 6-15).

Therefore it would have been obvious to one ordinary skill in the art at the time the invention was made to employ the teaching method of Ma method within the combination of Hashimoto and Weidner method in order to decrypt executable instructions simultaneously and access a core processor/instruction decoder (See Ma col.2 lines 3-5).

6. As per claim 2: the combination of Hashimoto-Weidner-Ma disclose the method wherein the encoding process is to discourage an attempt at recovering the private-state data from the storage by a process other than the decoding process (See Hashimoto 0035-0037, 0040).

7. As per claim 3: the combination of Hashimoto -Weidner-Ma disclose the method wherein the encoding process is only strong enough to cause an author of the software to apply, in writing said software, a technique prescribed by a manufacturer of the processor for accessing the private-state data from storage rather than circumventing said technique (See Hashimoto 0035-0037,0040,0082).

8. As per claim 4: the combination of Hashimoto -Weidner-Ma disclose the method wherein the private-state data refers to one of a) the content of an internal register of the processor that is not explicitly identified in an instruction manual for the processor that is intended for use by software developers (See Hashimoto Fig 1 step 2113 and 0036), and b) the content of an internal register of the processor that is explicitly identified in an instruction manual for the processor that is intended for use by software developers but is stored in one of a format and a location that is not explicitly identified in an instruction manual for the processor that is intended for use by software developers(See Hashimoto Fig 1 step 2113 and 0036).

9. As per claim 5: the combination of Hashimoto -Weidner-Ma disclose the method the method wherein the private-state data is written to one of a) a publicly accessible location in a register file of the processor (See Hashimoto Fig 1 step 2101 and 0036) b) cache (See Hashimoto Fig 3 step 152), and c) memory (See Hashimoto Fig 1 step 2103).

10. As per claim 6: the combination of Hashimoto-Weidner-Ma disclose wherein the encoding process is one in which the location of the written contents of a given internal register of the processor changes arbitrarily at least once, while repeating a)-b)(See Hashimoto 0038-0043).

11. As per claim 7: the combination of Hashimoto-Weidner-Ma disclose the method wherein the encoding process is one in which a storage format of the written contents of a given internal register of the processor changes arbitrarily at least once between big-endian and little-endian, while repeating a)-b)(See Hashimoto 0038-0043).

12. As per claim 8: the combination of Hashimoto-Weidner-Ma disclose the method wherein the encoding process is one in which a cipher is applied to the contents of a given internal register to produce an encoded value which is then written to the location in storage (See Hashimoto 0045).

13. As per claim 9: the combination of Hashimoto-Weidner-Ma disclose the method further comprising storing the decoded private state data in a private storage of the processor (See Weidner col.5 lines 12-32 and col. 4 lines 9-23).

14. Claims 10-33 are rejected under 35 U.S.C. 103(a) as being unpatentable over by EP 1,126,356(Kabushiki Kaisha Toshiba Aug 22,2001) in view of Weidner et al(hereinafter referred as Weidner) US Patent No 5,987,572.

15. As per claim 10: Hashimoto discloses an article of manufacture comprising: a data processing machine having a private internal state (See Hashimoto 0036, 0067), the internal state to change as the machine executes instructions provided to it as part of a program, wherein the machine is to encode data about the internal state and write the encoded state data to a location in a storage unit (See Hashimoto 0036).

Hashimoto does not explicitly teach the location being readable by software that is running on the machine.

However Weidner teaches the location being readable by software that is running on the machine (See col. 4 lines 7-35).

Therefore it would have been obvious to one ordinary skill in the art at that time the invention was made to employ the teaching method of Weidner within Hashimoto method in order to enhance security of the system.

16. As per claim 11: the combination of Hashimoto and Weidner disclose the article of manufacture wherein the data processing machine is a processor that has a special read micro-operation, to be used when the processor is to read said state data from the storage unit (See Hashimoto 0046,0040).

17. As per claim 12: the combination of Hashimoto and Weidner disclose the article of manufacture wherein the processor further includes an internal cache and is to also write the encoded state data to a public location in the cache (See Hashimoto Fig 3 step 152 and 0120).

18. As per claim 13: the combination of Hashimoto and Weidner disclose the article of manufacture wherein the processor is to recover the state data and write the recovered state data to a private location in the data processing machine (See Hashimoto 0037,0098).

19. As per claim 14: the combination of Hashimoto and Weidner disclose the article of manufacture wherein the processor is to recover the state data and configure itself with the recovered state data in preparation for resuming execution of a suspended task (See Hashimoto 0037,0098, 0129).

20. As per claim 15: the combination of Hashimoto and Weidner disclose the article of manufacture wherein the processor is one for which there is a manufacturer-defined instruction that, when executed by the processor, decodes and read the state data from the storage unit (See Weidner col. 5 lines 12-32 and col. 4 lines 9-23).

21. As per claim 16: the combination of Hashimoto and Weidner disclose the article of manufacture wherein the data processing machine is a processor for which a special micro-operation is defined for accessing the encoded state data from the storage unit, and wherein the processor further comprises an address obfuscation unit to receive an address value associated with given state data of the processor, the address value having been derived from a dispatch of the special micro-operation, the obfuscation unit to provide an encoded, physical address value that points to the actual location in the storage unit where the given state data is stored(See Hashimoto 0036-0037,0098,0129).

22. As per claim 17: the combination of Hashimoto and Weidner disclose the article of manufacture wherein the data processing machine is a processor for which a hardware control signal is defined for accessing the encoded data from the storage unit, and wherein the processor further comprises an internal cache, a data conversion unit to receive a data value from the internal cache as a result of a cache hit derived from the hardware control signal, the conversion unit to decode the data value into actual state data of the processor(See Hashimoto Fig 3 step 152 and 0120).

23. As per claim 18: Hashimoto discloses a computer system comprising: a processor (See 0064 and Fig 1 steps 2101); and a main memory communicatively coupled to the processor and having a public region designated to store the processor's private-state data in encoded form (See 0065-0066 and Fig1 steps 2101, 2103).

Hashimoto does not explicitly disclose wherein the instruction set architecture of the processor includes an instruction to decode and read the encoded private-state data form the public storage region.

However Weidner discloses wherein the instruction set architecture of the processor includes an instruction to decode and read the encoded private-state data form the public storage region (See col. 5 lines 12-32 and col. 4 lines 9-23)

Therefore it would have been obvious to one ordinary skill in the art at that time the invention was made to employ the teaching method of Weidner within Hashimoto method in order to enhance security of the system.

24. As per claim 19: the combination of Hashimoto and Weidner disclose wherein the processor encodes the private-state data prior to storing it to the public region (See Hashimoto 0036).

25. As per claim 20: the combination of Hashimoto and Weidner disclose wherein the processor decodes a value read from the public region prior to using it (See Weidner col. 5 lines 12-32 and col. 4 lines 9-23).

26. As per claim 21: the combination Hashimoto and Weidner disclose the system wherein the processor further includes an internal storage unit in which a public region is designated to store a copy of said private-state data in encoded form (See Hashimoto Fig 3 step 152 and 0120).

27. As per claim 22: the combination of Hashimoto and Weidner disclose the system wherein the internal storage unit is one of a cache and a register file (See Hashimoto Fig 3 step 152 and 0120).

28. As per claim 23: the combination of Hashimoto and Weidner disclose the system

wherein a private region is designated in the internal storage unit to store said private-state data in uuencoded form (See Hashimoto 0036, 0041).

29. As per claim 24: the combination Hashimoto and Weidner disclose the system further comprising a system chipset communicatively coupling the processor to the main memory (See Hashimoto Fig 1).

30. As per claim 25: Hashimoto discloses a method for operating a data processing machine, comprising: encoding private state data about a state of the machine (See 0036-0037); and writing, to a location in storage, the encoded private state data (0036-0037).

Hashimoto does not explicitly teach the location being readable by software that is running on the machine.

However Weidner teach the location being readable by software that is running on the machine (See col. 4 lines 7-35).

Therefore it would have been obvious to one ordinary skill in the art at that time the invention was made to employ the teaching method of within Hashimoto method in order to enhance security of the system.

31. As per claim 26: the combination of Hashimoto and Weidner disclose the method of wherein the encoding comprises ciphering a value of the private data to yield said encoded private data (See Hashimoto 0035-0037, 0040).

32. As per claim 27: the combination of Hashimoto and Weidner disclose the method wherein the private data about the state of the machine is one of a register value and a value from the storage (See Hashimoto 0035-0037, 0040).

33. As per claim 28: the combination of Hashimoto and Weidner disclose the method

wherein the encoding comprises address encoding to obfuscate an address value of the private data (See Hashimoto 0036).

34. As per claim 29: the combination of Hashimoto and Weidner disclose the method further comprising: recovering the private data from the storage according to a decoding process (See Hashimoto 0037, 0098).

35. As per claim 30: the combination of Hashimoto and Weidner disclose wherein the recovering comprises: reading a plurality of values from memory (See Hashimoto Fig 1 steps 115,152 and 0040-41); and combining the read plurality of values to form a single uuencoded value of said private data (See Hashimoto Fig 1 steps 115,152 and 0040-41).

36. As per claim 31: the combination of Hashimoto and Weidner disclose wherein the recovering comprises: reading a plurality values from one or more discontinuous locations of memory (See Hashimoto Fig 1 steps 115,152 and 0040-41); combining the read plurality values to form a single value ((See Hashimoto Fig 1 steps 115,152 and 0040-0041); and decoding the single value to form an uuencoded value of said private data (See Hashimoto Fig 1 steps 115,152 and 0040-41).

37. As per claim 32: the combination of Hashimoto and Weidner disclose the private data refers to one of a) the content of an internal register of the machine that is not explicitly identified in an instruction manual for the machine that is intended for use by software developers (See Hashimoto Fig 1 step 2113 and 0036), and b) the content of an internal register of the machine that is explicitly identified in an instruction manual for the machine that is intended for use by software developers but is stored in a format or location that is not explicitly identified in an instruction manual for the machine that is intended for use by software developers(See Hashimoto Fig 1 step 2113 and 0036).

38. As per claim 33: the combination Hashimoto and Weidner disclose further comprising storing the recovered private data in a private storage of the machine (See Hashimoto 0036-0037).

Conclusion

39. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. See PTO 892.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Fikremariam Yalew whose telephone number is 5712723852. The examiner can normally be reached on 9-5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Moazzami Nasser, can be reached on 571-272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-3852.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000

/Fikremariam Yalew/
Examiner, Art Unit 2436

12/14/2010

/Nasser Moazzami/
Supervisory Patent Examiner, Art Unit 2436